Journal of
Risk and Financial Management

MDPI

Article

Phishing Attacks on Cryptocurrency Investors in the Arab States of the Gulf

Marwa Alyami, Reem Alhotaylah, Sawsan Alshehri * and Abdullah Alghamdi

Information Systems Department, College of Computer Science and Information Systems, Najran University, Najran 61441, Saudi Arabia; 443306350@nu.edu.sa (M.A.); 443306360@nu.edu.sa (R.A.); aaalghamdi@nu.edu.sa (A.A.)
* Correspondence: 443306357@nu.edu.sa

Abstract: With the rapid development of technology in all fields, including the financial field, people have flocked to invest in cryptocurrencies, sometimes without prior knowledge or experience. This has prompted hackers to prey on inexperienced investors through many types of fraud and attacks, especially phishing attacks. Cryptocurrency investment transactions take place without intermediaries such as banks and monetary institutions. Investing in cryptocurrencies is a form of peer-to-peer transaction and takes place without the involvement of physical wallets. This study addresses cases where people may become victims of phishing attacks due to the nature of cryptocurrency investments. The aim of this study was to understand the concepts of various phishing attacks on cryptocurrencies and to measure the awareness of cryptocurrency investors in the Arab Gulf countries regarding the security risks associated with cryptocurrency investments. This research was conducted by distributing a questionnaire among cryptocurrency investors and collecting and analyzing all the survey responses. The results reveal a lack of awareness about how to deal with the security risks associated with cryptocurrency investments. The research concludes that the majority of cryptocurrency investors are unaware of how to deal with phishing attacks. Finally, we address future research directions and recommend actions that can be taken to increase investors' awareness of this issue.

Keywords: cryptocurrencies; investors; awareness; investing; cybersecurity; social engineering; phishing attacks; fraud

Citation: Alyami, Marwa, Reem Alhotaylah, Sawsan Alshehri, and Abdullah Alghamdi. 2023. Phishing Attacks on Cryptocurrency Investors in the Arab States of the Gulf. *Journal of Risk and Financial Management* 16: 271. https://doi.org/10.3390/jrfm16050271

Academic Editor: Badar Nadeem Ashraf

Received: 28 March 2023
Revised: 9 May 2023
Accepted: 10 May 2023
Published: 13 May 2023

1. Introduction

With the spread of technology, people have become consumed with keeping abreast of all things modern and fast. Recently, the concept of investing in cryptocurrencies has spread, and there has been a rise in the number of cryptocurrency users on investment platforms, with people rushing to make use of it and earn money faster.

Cryptocurrency exchange on electronic investment platforms refers to the effective, direct exchange of an asset between people without the intervention of a central authority that guarantees their rights and checks their transactions. The primary motivation behind the establishment of cryptocurrencies was to create a peer-to-peer cash exchange system, as this process is performed using cryptography to secure transactions, without the need for a trusted authority such as a central bank; instead, it uses a decentralized system to record transactions and issue new units.

Since its establishment, the popularity of cryptocurrency exchange among the public has been high, and cryptocurrency platforms have paved the way for attackers to exploit inexperienced people who want to make a quick profit; these people are attractive targets for hackers.

Attackers take advantage of the idea that the identities of users of cryptocurrency platforms can be faked, which increases their chances of escaping arrest and reduces the

possibility that they will be legally punished for undertaking fraud and exploitation; this idea has contributed to the implementation of a group of large-scale and varied electronic attacks on exchanges, especially social engineering attacks such as phishing. According to an earlier scientific study, the percentage of fraudulent cryptocurrency exchanges was 83%, and phishing was the second largest category after referral fraud (when an attacker uses dishonest techniques to exploit people who use referral programs), with a percentage of 26.65% (Xia et al. 2020a).

Additionally, phishing is one of the most prominent and dangerous social-engineering-related electronic attacks to occur on digital currency platforms. It is a type of cyberattack involving an attempt by an unauthorized person to access a victim's private and sensitive information, whereby the victim is deceived and lured by the attacker, who gains the victim's trust, hoping to obtain their personal data and property. Attackers can include fake personal information and have the ability to make this information appear realistic; moreover, they can create fake advertisements or send deceptive emails that appear official and legal. This leads users to believe that the attacker is a trusted party with whom they can conduct cryptocurrency investment and exchange.

In recent years, researchers have continued to evaluate safe investment in cryptocurrencies, and have made efforts to propose technical solutions and raise awareness. Such solutions aim to address or limit the damage caused by the spread of phishing attacks in such transactions because of their anonymous nature. Most of the research that is concerned with measuring the awareness of investors does not specify the Arab States of the Gulf, which has created a research gap.

This study contributes to the literature in the following ways. First, we measure the awareness of cryptocurrency investors in the Arab States of the Gulf regarding phishing attacks. Secondly, possible reasons for deficiencies in awareness and knowledge of safe cryptocurrency investment are identified and explained. Third, a number of solutions are proposed that can be implemented by the responsible authorities, or by the investors themselves, to handle this type of cyberattack. In short, this study highlights and measures the extent to which cryptocurrency investors in the Arab States of the Gulf are aware of secure transactions and measures their likelihood of falling victim to phishing attacks.

This paper investigates cryptocurrency exchange phishing cases, the security issues associated with cryptocurrency investment, how people become victims of it, and their knowledge of how to avoid becoming phishing attack victims. We achieved these aims by reviewing previous literature on the latest cybercrimes related to phishing attacks on cryptocurrencies, disseminating a questionnaire to several community groups for cryptocurrency investors in the Arab States of the Gulf, and then analyzing the answers to determine the fraud-related issues and problems faced by those investors. The responses emphasized the need for cryptocurrency investors to improve their security awareness.

This research is organized as follows: Section 2 discusses previous papers on investing in cryptocurrencies in general, phishing and fraud methods, and some previously proposed solutions. Section 3 discusses the methodology used in this research, which involved an online questionnaire distributed among cryptocurrency investors in the Arab States of the Gulf. Section 4 shows a statistical analysis of the results of the published questionnaire and discusses the findings with regard to the research questions. Section 5 outlines some recommendations, as well as final comments, summarizing findings and offering guidance for future work.

Research Questions

The primary goal of this paper was to study the threats and dangers of phishing attacks on cryptocurrency investors in the Arab States of the Gulf, as guided by the following research questions (RQs):

RQ1: Are phishing attacks the most common type of attack on cryptocurrency?

RQ2: What phishing methods might occur?

RQ3: What is the impact of phishing attacks?

RQ4: Do cryptocurrency users in the Arab States of the Gulf have sufficient knowledge about each cryptocurrency's background and their related projects?

RQ5: How aware are investors of cryptocurrencies of the dangers of phishing attacks?

After determining the research questions, the second step was to review the previous literature.

2. Literature Review

In this section, we review the literature that has informed this paper. The first section focuses on the general concept of cryptocurrency technology. The second section summarizes fraud, specifically phishing in the cryptocurrency community and on its platforms, and discusses the issues and problems caused by this type of phishing. The third section summarizes the methods and solutions that can be used to avoid the phishing fraud that exists on cryptocurrency platforms and in its communities.

2.1. Cryptocurrency Definition

Cryptocurrencies are digital assets that exist to create intangible money based on blockchain technology and were invented in 2008 (Xia et al. 2020a). They provide and manage data warehouses without a central governing system and aim to ensure the safety of their inputs via encryption, making it difficult to change these inputs (Lal et al. 2021).

Investors generate these currencies through a series of numbers and letters and then transfer them between devices through private and public keys (Reddy 2020). When an investor wants to make a deal, they must have one of two pairs of digital keys. Once the investor executes the transaction, it cannot be modified or retrieved (Trozze et al. 2022).

There are two ways to store these cryptocurrencies: in a hot wallet (online) or a cold wallet (offline) (Trozze et al. 2022). These features of blockchain technology (its use of intangible assets, decentralization, the lack of a requirement for users to provide a real identity, and the absence of a judicial authority) have created an ideal environment for cybercrime (Astrakhantseva et al. 2021).

2.2. Cryptocurrency Fraud and Phishing

Cryptocurrencies are decentralized as they do not depend on official authorities, government, or banks, thus facilitating cybercrime such as fraud, theft, the unauthorized use of computer resources (for mining), and social engineering attacks (to steal credentials), as well as providing criminals with opportunities to commit new crimes (Reddy and Minnaar 2018; Lapuh Bele 2021; Corbet et al. 2020).

Perhaps the most important feature that blockchain investing platforms provide is anonymity, whereby the investor, whether a hacker or an ordinary person, does not disclose their identity. This attracts hackers, who use it as a means to contact their victims under false pseudonyms in order to deceive them and gain their trust (Lal et al. 2021).

Social engineering is the main attack in the cryptocurrency community and has become increasingly common (Ivanov et al. 2021; Weber et al. 2020); it involves attackers using psychological tricks that enable them to gain access to the contents of users' wallets (Weber et al. 2020). Cryptocurrency phishing is the most common technique used in social engineering techniques. It includes any phishing threat that seeks to reveal sensitive information and gain cryptocurrency using mail, ads, social media sites, and text messages (Sayeed and Marco-Gisbert 2018; Froehlich et al. 2021). Phishing incidents also accounted for 98% of social incidents in 2018 (Andryukhin 2019). According to a study that took place in 2019 on the famous Binance platform, a group of thieves took cryptocurrencies worth 7000 Bitcoins, which is equivalent to USD 41 million today, by carrying out fraudulent attacks, including phishing (Holub and O'Connor 2018).

Attackers seek to obtain the private keys or credentials of the cryptocurrency user in phishing, which occurs in many ways, the most common being through Punycode or fake airdrops. Punycode sends an email to the user by falsifying the email address and domain of an official website, and prompts the user to enter the required data on the official site.

Fake airdrops are more accurate forms of phishing whereby the attacker asks the user for all of the required data (email and wallet information) by imitating an official platform for the exchange of money between wallets, whether via email or a social networking site (Astrakhantseva et al. 2021).

Credential phishing is one of the biggest security issues on the internet, and attackers have found cryptocurrency phishing to be a very profitable type of attack (Wen et al. 2021). One of the reasons that a hacker was able to steal the equivalent of nearly USD 50 million in cryptocurrency on investing platforms could be the difficulty of detecting the phishing attacker who targeted Ethereum (Badawi and Jourdan 2020; Gottipati 2020).

Coinhoarder is a famous Bitcoin phishing campaign that occurred in 2017 in Ukraine, whereby almost USD 115 million was reported to be stolen from Ethereum users. During this attack, the attackers stole tens of millions of dollars by making their phishing pages appear as official pages through the illegal use of fake SSL certificates (Holub and O'Connor 2018).

Cryptojacking attacks are a famous issue in cryptocurrency, in which computer resources (processor, etc.) are accessed in many ways, one of which is through phishing, which is a common way for attackers to initiate mining operations (Varlioglu et al. 2022). Additionally, on the dark web, services for presenting pages and disguised phishing documents (invoices, etc.) are sold (Șcheau and Zaharie 2018).

Ignorance is one of the problems that make users fall victim to phishing. Users do not have enough knowledge of cryptocurrencies or enough security awareness. They interact with phishing sites that look legitimate and send their coins to attackers' wallets (Ahvanooey et al. 2021).

Finally, due to the expansion of digital currencies during the COVID-19 crisis and the increase in the number of new users, companies were prompted to start accepting digital currencies as payment, therefore making cryptocurrency phishing one of the most common and growing forms of fraud during this time (Xia et al. 2020b).

The previous literature includes various forms of phishing, either direct or indirect, as phishing is a means of carrying out other attacks and crimes on/using cryptocurrencies. Recognizing these types of attacks can enable us to identify ways to prevent and recover from them.

2.3. Methods and Results

The Internet is a constantly growing environment and provides complex and difficult tools. Therefore, it is necessary to impose preventive and defensive measures worldwide, to prevent and mitigate such cybercrimes on cryptocurrencies, and to reduce phishing attacks.

Șcheau and Zaharie believe that cryptocurrencies hold both promising and negative potential for the future (Șcheau and Zaharie 2018). Researchers used machine learning to highly accurately detect suspicious activity in transactions, and thus, detect phishing attacks after analyzing the periodic behavior of transactions (Lal et al. 2021). As for other researchers' proposed solutions, AdaBoost classifiers are used to detect malicious entities, and it was determined that its features were effective in doing so (Poursafaei et al. 2020).

Due to the lack of user knowledge about cryptocurrency, it has been suggested that Runtime Application Self-Protection (RASP) be used, which is a cyber security technique and a security tool. This works by detecting an attack according to vulnerabilities in the code and by observing the behavior of the application in real time rather than relying on predefined patterns or signatures. It is also used with a Hardware Security Module (HSM), to provide protection during the exchange of cryptocurrencies (Gottipati 2020) (see Figure 1).

Researchers categorized six types of threats to cryptocurrency, and suggested countermeasures for each threat. One of the threats was phishing, and its countermeasures included: opening the URL of the legitimate system directly, using multiple authentications, and using a cold wallet (Froehlich et al. 2021).

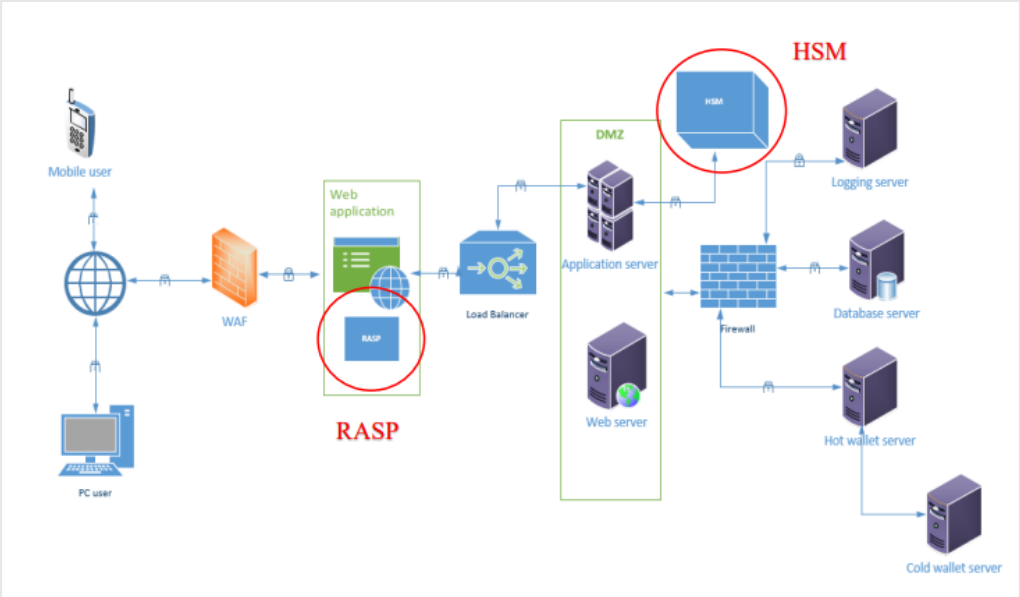

Figure 1. RASP and HSM for cryptocurrency exchange.

Researchers analyzed public online and blockchain-based data and created a classification system for scams with pre-charged scams. DBSCAN (Density-Based Spatial Aggregation for Applications with Noise) technology was applied to these data (Chen et al. 2020). This is a machine learning algorithm that detects different shapes and sizes of datasets that contain outliers. Additionally, it was applied to the detection of fraudulent websites and malicious websites. The results showed that the ranking found sixteen phishing sites out of a thousand scam sites (Phillips and Wilder 2020).

Meanwhile, other researchers analyzed the most-used schemes in phishing attacks on blockchains, recommended a form of defense against these schemes, and made alternatives to the DNS used in phishing (Andryukhin 2019).

A framework has been developed for phishing detection based on the use of social engineering. By referring to records of agreements and transactions, this framework performs three steps on Ethereum, and aims specifically to find phishing attacks, starting with a thorough search of criminals' transaction histories. Then, the criminals' accounts are found directly on Ethereum, rather than through their scam methods and messages (Badawi and Jourdan 2020). Meanwhile (Yuan et al. 2020), researchers have proposed detecting phishing in Ethereum blockchain transactions by means of algorithms that effectively detect phishing using etherscan.io client and crawling, and then, aggregating all the phishing transactions and addresses. Next, the researchers created a transaction graph and suggested a way to extract the progression feature based on the graph.

Additionally, a framework that automatically recognizes cryptocurrency fraud has provided new insights into future exposure work on Ethereum (Bartoletti et al. 2021). Moreover, 1000 phishing nodes were processed to advance the development of phishing fraud detection and improve blockchain security through data structures and representative structures of node features in the technology in the network (Chen et al. 2021). A classification system has also been developed for two phishing addresses on two approved sites: trans2vec; this is a classification system that aims to find and report address sequences, to find and identify possible future phishing attacks (Wu et al. 2022).

Another group of authors evaluated Ethereum's security and anti-phishing tools using 200 phishing URLs and 500 legitimate URLs, using ten phishing tools for evaluation; and they found that just one of these tools could perform accurate identification of over 90% of the phishing URLs (Dika and Nowostawski 2018).

Researchers have provided a new a priori method for detecting user groups that are likely to be involved in P&D schemes. The Mt. Gox confirmed the leaked algorithm's

validity using the Bitcoin exchange's transaction history, through which many suspicious investing practices were discovered (Chen et al. 2019).

Legally, cryptocurrency is data. Thus, one of the provisions of the Information Crimes Act in South Africa was to criminalize the possession data illegally obtained through phishing and other attacks, and perpetrators of this crime are prosecuted (Reddy 2020). Moreover, the Criminal Code of the Russian Federation punishes those who perform phishing to access protected computer data with the aim of copying, destroying, or modifying the content of the cryptocurrency (Trozze et al. 2022).

Arab researchers analyzed the real challenges pertaining to currencies in Arab countries and found that digital currency has not been recognized in the Arab community because of the terms of religion, a lack of approval from Governments, and the cost of the Internet (Shetewy et al. 2019).

The literature is limited to the technical and legal aspects of combating phishing in cryptocurrency, and awareness among users has not received sufficient attention.

In this paper, we compared thirty-one papers from six aspects (cryptocurrency, phishing, techniques, suggested solutions, and contact with investors), as shown in Figure 2. Through this, we discovered the limitations of previous studies and their focus on specific aspects but not others. We cover the six abovementioned aspects in this paper in order to find and analyze the most important causes of fraud and then deduce the appropriate solution.

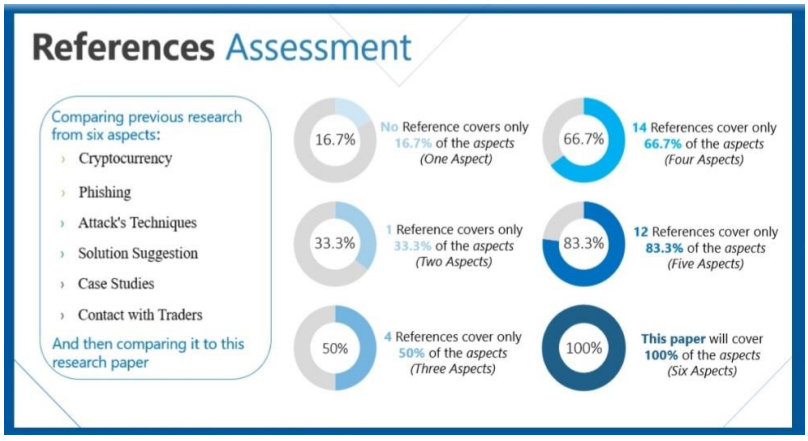

Figure 2. Reference assessment.

3. Methodology

This study was cross-sectional and used a questionnaire, conducted in April 2022. The target audience were investors in cryptocurrency in the Arab States of the Gulf, who amount to a total number of about 747,100, according to statistics. The pools and channels of cryptocurrency investors were searched on the social media platforms Twitter and Telegram, and the total number of these investors on pools and channels was 250,000. An electronic the technique was used to collect data, the number of investors approached was 970, and the final number of respondents was 614 (a response rate of 63.3); we excluded both responses that were given in the trial period of the questionnaire and the responses of non-Gulf citizens, with 241 non-Gulf citizen respondents and 115 responses given in the trial period.

The data were gathered from each platform over two consecutive weeks; in the first week, they were collected from the Telegram platform, and in the second week, from Twitter platform. Influencers in these communities cooperated with us to publish the survey. We also obtained admin approval for each channel and grouped the channels before publishing the survey. We interacted with the participants in groups during the process, in case there was a need to clarify specific questions, and asked them to answer with credibility.

We sent the survey to several WhatsApp group investors before it was officially published and asked for feedback regarding the questions' clarity and comprehensiveness.

The feedback was considered, and the survey was improved and published in its final form. The data collected in the trial period were excluded—as mentioned earlier—which included 115 responses. The survey contained 14 questions divided into 3 sections, which were as follows: The first section included three questions about the survey participants' personal information, such as gender, age group, and country of residence (since we targeted cryptocurrency communities in the Arab States of the Gulf). The second section included questions about the participants' knowledge of cryptocurrencies and how to use their systems and platforms, and included a question that assessed people's knowledge of dealing with these platforms and cryptocurrencies. The third section contained questions about exposure to fraud in terms of its forms. The questionnaire was presented with the integration of Arabic and English, as there are English terms in cryptocurrencies that cannot be translated into Arabic.

It was challenging to identify the characteristics of investors since most of them did not use their real identities while taking the questionnaire and taking part in the interviews. However, there were some similarities and differences among investors. The predominant age group was young people; we assume that this is because they are at the beginning of their careers and seek to increase their basic income, as most of them were employers. Additionally, most of the sample were Saudi Arabians, as they form most of the population in the Arab Gulf states. Male investors formed the majority of the sample, as for decades, women were not allowed to manage their money without a man's approval, according to Career Group Companies. Another reason for this disparity is the gender pay gap. The average wage of males is higher than that of females, as reported by the Saudi newspaper Al-Watan (Ali 2021).

The interviews also showed that most of the investors had already invested in the stock markets and relied more on investing in stocks than investing in cryptocurrencies. It became clear from interviews with officials that investors are very interested in technology, as for some, cryptocurrency offers an opportunity to delve deeper into technology.

4. Statistical Analysis

The characteristics of our respondents were described using frequency distribution, and we also used the Chi-square test to examine the distribution of cryptocurrency phishing attack methods to which investors fall victim, according to the demographics. We used a p-value of less than 0.05 as the cut-off level for statistical significance.

4.1. Results

Table 1 displays the demographic characteristics and the personal information of our final respondents, and the data rates for the questions in the first section that refer to the personal information of the respondents, such as age, gender, and country (since we targeted cryptocurrency communities in the Arab States of the Gulf). In general, the majority of respondents were men (85%) and from Saudi Arabia (83.5%).

Table 2 shows the proportions of answers to questions about investors' experiences and their ways of dealing with cryptocurrencies. Most of the respondents expect a high rate of cryptocurrency use in their country in the future (86.3%), and we found that about 50.8% prefer using decentralized platforms. Decentralized platforms use peer-to-peer transactions between investors, without the intervention of an intermediary, such as banks and monetary institutions. The reason that that users prefer decentralized platforms is that it allows them to have more control of their transactions.

However, the majority of respondents use Binance, as it is one of the most popular cryptocurrency exchanges and ensures that investors are investing in a reliable platform. Despite being a centralized platform, which means that this platform acts as an intermediary between investors and will make money through transactions fees, it has an average rate of 82.7%.

Table 1. Demographic characteristics of the respondents (N = 614).

Variable	N (%)
Gender	
Male	522 (85%)
Female	92 (15%)
Age	
18–25	110 (17.9%)
26–40	396 (64.5%)
41–60	100 (16.3%)
Older than 60	8 (1.3%)
Country	
Saudi Arabia	513 (83.5%)
UAE	27 (4.4%)
Oman	11 (1.8%)
Qatar	7 (1.1%)
Kuwait	44 (7.2%)
Bahrain	12 (2%)

With most respondents trusting global platforms when investing in cryptocurrencies, the average of 81.1% is due to the popularity of global platforms, which are the oldest. We also found that most respondents use a hot wallet to store their cryptocurrency instead of a cold wallet (83.2%); this makes them vulnerable to fraud, because a hot wallet is considered less secure compared to a cold wallet, which has no internet connection.

A total of 39.25% of cryptocurrency investors had previously been scammed while investing, because they invested impulsively and with little knowledge. The highest rate was for email scams because it is one of the most commonly used methods of phishing, and users consider messages more trustworthy if they receive them via email, on social media, or on a platform page promoting fake investing.

Table 2 displays the percentage of data for each answer to the questions of the second section of the questionnaire, which pertains the experience of investors and their methods of dealing with cryptocurrencies.

Table 3 shows the proportions of answers to questions related to knowledge about cryptocurrencies and how their systems and platforms are used, and includes a question that measures people's knowledge of how to deal with these platforms and currencies. Regarding the respondents' opinions of cryptocurrencies (knowledge, difficulty, awareness, security, and possibility of fraud), their percentages were 35.3%, 70.3%, 36.7%, 66.8%, and 33%, respectively, whereas their knowledge of cryptocurrency was less than half, at 35%; this is an unfavorable percentage and an indication that investors rush in and take risks without enough knowledge, rendering them vulnerable to fraud.

On the other hand, respondents indicated that they face difficulty in using and dealing with cryptocurrencies, as the difficulty percentage was 70.3%. In terms of awareness, 36.7% were security aware, which makes sense given the lack of deliberation prior to investing. As for the perceived safety of investing, the percentage was 66.8%, indicating that the participants feel safe while investing and ignore the role of increasing security due to their lack of awareness.

As for the probability of being scammed, the percentage was 33%, which is a somewhat contradictory result when considering the participants' lack of knowledge regarding investing. We do not consider this an accurate percentage, as participants may not have previously been exposed to a disguised phishing email impersonating a trusted platform, leading them to believe that they are not vulnerable to fraud.

Tables 4–6 show the percentages of each demographic group compared to each other. Most of the respondents, according to their gender, were in the age group 26–40, with 67% being males and 50% females, and the majority were from the Kingdom of Saudi Arabia, with 83.7% being males and 82.6% females. When calculating the percentages of

the demographic groups according to age, it appeared that the majority were males (76.3% in the 18–25 age group, 88.4% in the 26–40 age group, and 85% in the 41–60 age group). Except for the age group over 60, most respondents were female (62.5%), and most of the respondents were from the Kingdom of Saudi Arabia (80% for the age group 18–25, 85.9% for the age group 26–40, 79% for the age group 41–60, and 75% for the age group above 60). Finally, when calculating the percentages of the demographic groups by country, we found that most of the respondents, according to their countries, were male, with a percentage of 85.2% for the Kingdom of Saudi Arabia, 74.1% for the UAE, 90.9% for Oman, 85.7% for Qatar, 90.9% for Kuwait, and 75% for Bahrain. Most of these respondents, according to their countries, were in the age group 26–40, with a percentage of 66.3% for the Kingdom of Saudi Arabia, 59.3% for the UAE, 63.6% for Oman, 42.9% for Qatar, 56.8% for Kuwait, and 41.7% for Bahrain.

Table 2. Investors' experiences and methods of dealing with cryptocurrency (N = 614).

Variable	N (%)
High Expectation of Cryptocurrency Usage	
Yes	530 (86.3%)
No	18 (2.9%)
Maybe	66 (10.7%)
English Language as an Obstacle	
Yes	231 (37.6%)
No	370 (60.3%)
Maybe	66 (2.1%)
Platform System	
Centralized platforms	302 (49.2%)
Decentralized platforms	312 (50.8%)
Used Arabic Trading Platform	
Coinmena	67 (10.9%)
Rain	182 (29.6%)
Bitoasis	94 (15.3%)
Others	271 (44.2%)
Used Trading Platform	
Coinbase	13 (2.1%)
Binance	508 (82.7%)
Bitfinex	14 (2.3%)
Kucoin	49 (8%)
Others	30 (4.9%)
Trusted Platforms	
Arabic platform	116 (18.9%)
Global platform	498 (81.1%)
Wallet type	
Hot	511 (83.2%)
Cold	103 (16.8%)
Phishing and Scam Methods (from 240 answers)	
Via email or social networking sites	46 (19.2%)
Fake trading platform page	43 (17.9%)
Electronically, such as via malicious links	35 (14.6%)
Google adware	37 (15.4%)
Fake mobile apps	17 (7.1%)
Fake education websites	34 (14.2%)
Automated trading (boot)	21 (8.8%)
Other answers	7 (2.8%)

Table 3. Measuring people's knowledge of dealing with cryptocurrencies (N = 614).

	N (%)				
Question	**Very High**	**High**	**Moderate**	**Little**	**Very Little**
How much do you know about cryptocurrency?	88 (14.3%)	129 (21%)	316 (51.5%)	66 (10.7%)	15 (2.4%)
How difficult is it to exchange cryptocurrency?	57 (9.3%)	139 (22.6%)	236 (38.4%)	121 (19.7%)	61 (9.9%)
The extent of awareness you have of the background and credibility of each currency and the projects based on it before	82 (13.4%)	143 (23.3%)	268 (43.6%)	86 (14%)	35 (5.7%)
According to your opinion and through your own experience, what is your assessment of the level of security provided by cryptocurrency platforms?	145 (23.6%)	265 (43.2%)	166 (27%)	27 (4.4%)	11 (1.8%)
Possibility of being scammed on cryptocurrency exchanges	98 (16%)	111 (18.1%)	202 (32.9%)	112 (18.2%)	91 (14.8%)

Table 4. Statistics related to age and country based on each gender.

Variable	**Gender**	
	Male N = 522 (%)	**Female N = 92 (%)**
Age		
18–25	84 (16.1%)	26 (28.3%)
26–40	350 (67%)	46 (50%)
41–60	85 (16.3%)	15 (16.3%)
Older than 60	3 (0.6%)	5 (5.4%)
Country		
Saudi Arabia	437 (83.7%)	76 (82.6%)
UAE	20 (3.8%)	7 (7.6%)
Oman	10 (1.9%)	1 (1.1%)
Qatar	6 (1.1%)	1 (1.1%)
Kuwait	40 (7.7%)	4 (4.3%)
Bahrain	9 (1.7%)	3 (3.3%)

Table 5. Statistics related to gender and country based on each age.

Variable	**Age**			
	18–25 N = 110 (%)	**26–40 N = 396 (%)**	**41–60 N =100 (%)**	**Older than 60 N = 8 (%)**
Gender				
Male	84 (76.4%)	350 (88.4%)	85 (85%)	3 (37.5%)
Female	26 (23.6%)	46 (11.6%)	15 (15%)	5 (62.5%)
Country				
Saudi Arabia	88 (80 %)	340 (85.9%)	79 (79%)	6 (75%)
UAE	4 (3.6%)	16 (4%)	6 (6%)	1 (12.5)
Oman	3 (2.7%)	7 (1.8%)	1 (1%)	0 (0%)
Qatar	1 (0.9%)	3 (0.8%)	3 (3%)	0 (0%)
Kuwait	10 (9.1%)	25 (6.3%)	9 (9%)	0 (0%)
Bahrain	4 (3.6%)	5 (1.3%)	2 (2%)	1 (12.5%)

Table 6. Statistics related to gender and age based on each country.

Variable	Country					
	Saudi Arabia N = 513 (%)	UAE N = 27 (%)	Oman N = 11 (%)	Qatar N = 7 (%)	Kuwait N = 44 (%)	Bahrain N = 12 (%)
Gender						
Male	437 (85.2%)	20 (74.1%)	10 (90.9%)	6 (85.7%)	40 (90.9%)	9 (75%)
Female	76 (14.8%)	7 (25.9%)	1 (9.1%)	1 (14.3%)	4 (9.1%)	3 (25%)
Age						
18–25	88 (17.2%)	4 (14.8%)	3 (27.3%)	1 (14.3%)	10 (22.7%)	4 (33.3%)
26–40	340 (66.3%)	16 (59.3%)	7 (63.6%)	3 (42.9%)	25 (56.8%)	5 (41.7%)
41–60	79 (15.4%)	6 (22.2%)	1 (9.1%)	3 (42.9%)	9 (20.5%)	2 (16.7%)
Older than 60	6 (1.2%)	1 (3.7%)	0 (0%)	0 (0%)	0 (0%)	1 (8.3%)

When comparing the distribution of crypto phishing tactics among investors according to demographics (gender, age, and country), we found a significant association with awareness and a higher rate of female scam victims, possibly because females are more trusting than males (56.7%, 36%, $p < 0.05$). The age group most exposed to phishing attacks was the over-60 age group (87.5%) as they lack knowledge of reliable methods for checking messages and phishing methods, and they are less knowledgeable and less vigilant about technology than cryptocurrency investors. The highest percentage of investors exposed to phishing attacks was among investors from Oman, with an average of 63.6%. For example, only 28.6 percent of investors in Qatar experienced phishing attacks when dealing with cryptocurrencies, while 58.3 percent, 55.6 percent, 40.9 percent, and 37.2 percent of investors in Bahrain, the UAE, Kuwait, and Saudi Arabia, respectively, disclosed phishing attacks when dealing with cryptocurrencies. The general level of awareness of dealing with cryptocurrencies was not sufficient for 240 investors (39.25%) because they were victims of cryptocurrency phishing attacks, while 371 investors (60.75%) had a good level of awareness and were able to avoid phishing attacks, as shown in Table 7.

Table 7. Distribution of phishing methods among cryptocurrency investors according to demographics.

Variable	Cryptocurrency Investors as Victims of Phishing Score		
	Yes N (%)	No N (%)	*p*-Value
Gender			
Male	188 (36%)	334 (64%)	X^2 (1, N = 614) = 13.814, $p = 0.0002$
Female	52 (56.7%)	40 (43.3%)	
Age			
18–25	48 (43.36%)	62 (56.64%)	X^2 (3, N = 614) = 9.503, $p = 0.0233$
26–40	148 (37.4%)	248 (62.6%)	
41–60	37 (37%)	63 (63%)	
Older than 60	7 (87.5%)	1 (12.5%)	
Country			
Saudi Arabia	191 (37.2%)	322 (62.8%)	X^2 (5, N = 614) = 8.303, $p = 0.140$
UAE	15 (55.6%)	12 (44.4%)	
Oman	7 (63.6%)	4 (63.4%)	
Qatar	2 (28.6%)	5 (71.4%)	
Kuwait	18 (40.9%)	26 (59.1%)	
Bahrain	7 (58.3%)	5 (41.7%)	

4.2. Discussion

In this study, possible reasons for the deficiencies in awareness and knowledge of safe investment in cryptocurrency are found and explained. Based on the results of our electronic survey distributed among investors in the Arab Gulf countries, we have found

answers to the research question that prompted us to conduct this research. Our question concerned whether phishing attacks are the most common type of cryptocurrency attack; we found that it is. Phishing attacks are the most common type of social engineering attack on cryptocurrencies, and social engineering attacks in general are the most common type of cyberattack on cryptocurrencies. As we were curious to know the most common ways in which phishing occurs, we investigated this and found that it occurs through fake platforms, misleading emails, and false advertisements. Additionally, in our research on the effects of phishing attacks, the most common negative outcome for cryptocurrency investors was the theft of their cryptocurrency.

We were interested in seeing whether cryptocurrency users in the Arab Gulf countries are sufficiently knowledgeable about the background of each cryptocurrency and their related projects (for which we found a value of 35%). Additionally, our quest to find out how aware cryptocurrency investors are of the risks of phishing attacks seems to be insufficient knowledge about the risk of phishing attacks, as 39.25% of cryptocurrency investors have been scammed previously.

5. Conclusions

In conclusion, the focus of this paper was on awareness when investing in cryptocurrencies in the Arab States of the Gulf. To this end, we studied the threat and danger of phishing on cryptocurrencies via a literature review of thirty-one scientific papers, and the methodology involved a questionnaire for the targeted audience (investors in cryptocurrencies in the Arab States of the Gulf), which revealed that the majority of investors did not have sufficient awareness of cryptocurrencies and investing in them.

Moreover, the results revealed heavy phishing attacks. This emphasizes the importance of investors having sufficient awareness before and during investing to avoid falling a victim to various types of phishing, as well as full background knowledge of cryptocurrencies, self-education, and greater interest from the concerned authorities in the danger of cryptocurrency fraud, as these will improve investor awareness.

In future work, we recommend raising awareness among these investors across all platforms and websites to develop methods that will enable them to avoid becoming victims of phishing. Additionally, we recommend that investors have complete knowledge of the appropriate investing methods for dealing with the exchange of cryptocurrencies, because once the transaction is executed, no modification or refund can occur.

It is recommended that investors receive extensive training on all platforms and websites before and whilst they deal with other investors. Such training will improve investors' abilities to identify unreliable investors and attackers, as well as understand the importance of verification before conducting investing transactions. Additionally, it is important to be aware of the different methods of phishing attacks, as has been mentioned in previous research (Rubia Fatima et al. 2019). The authors mention strategies that use game techniques, such as the PhishI game, to learn about phishing attacks. Additionally, the authors mention risks associated with excessive online exposure and recommend using game scenarios to develop security requirements.

Consequently, focusing on such methods to develop strategies against social engineering and phishing attacks is recommended.

The results of this study may help in the development of supportive technical solutions, such as machine learning solutions and methodologies, to detect cryptocurrency phishing. Moreover, we hope that it will encourage Arab researchers to show sufficient interest in this fast-spreading problem, to reduce such attacks and spread adequate awareness of how to avoid them. Additionally, we hope that our results will serve as a catalyst for improving the legislation of various countries. Trading in cryptocurrencies requires more global attention and should be improved through the enactment of legal policies that limit incorrect practices that expose investors to fraud or prevent the preservation of public interest.

Author Contributions: Conceptualization, M.A., R.A. and S.A.; methodology, M.A., R.A. and S.A.; validation M.A., R.A. and S.A.; formal analysis, M.A., R.A. and S.A.; resources, M.A., R.A. and S.A.; data curation M.A., R.A. and S.A.; writing—original draft preparation, M.A., R.A. and S.A.; writing—review and editing, M.A., R.A. and S.A.; visualization, M.A., R.A. and S.A.; supervision, A.A.; project administration, A.A.; funding acquisition, A.A. All authors have read and agreed to the published version of the manuscript.

Funding: The authors are thankful to the Deanship of Scientific Research at Najran University for funding this work under the Future Funding program (grant code NU/SRP/SERC/12/3).

Data Availability Statement: The data that support this study are available from the author upon reasonable request.

Conflicts of Interest: The authors declare no conflict of interest.

References

Ahvanooey, Milad, Wojciech Mazurczyk, Mark Zhu, Max Kilger, and Kim-Kwang Choo. 2021. Do Dark Web and Cryptocurrencies Empower Cybercriminals? Paper presented at the 12th EAI International Conference on Digital Forensics Cyber Crime, Virtual Event, Singapore, December 6–9; vol. 441, pp. 277–93. [CrossRef]

Ali, Zina. 2021. The Salary Gap Is Irregular Differences between the Genders. Al-Watan. Available online: https://www.alwatan.com.sa/article/1068497 (accessed on 26 March 2022).

Andryukhin, A. A. 2019. Phishing Attacks and Preventions in Blockchain Based Projects. Paper presented at the 2019 International Conference on Engineering Technologies and Computer Science: Innovation and Application, EnT 2019, Moscow, Russia, March 26–27; pp. 15–19. [CrossRef]

Astrakhantseva, Irina, Roman Astrakhantsev, and Alexey Los. 2021. Cryptocurrency fraud schemes analysis. *SHS Web of Conferences* 106: 02001. [CrossRef]

Badawi, Emad, and Guy-Vincent Jourdan. 2020. Cryptocurrencies emerging threats and defensive mechanisms: A systematic literature review. *IEEE Access* 8: 200021–37. [CrossRef]

Bartoletti, Massimo, Stefano Lande, Andera Loddo, Livio Pompianu, and Sergo Serusi. 2021. Cryptocurrency scams: Analysis and perspectives. *IEEE Access* 9: 148353–73. [CrossRef]

Chen, Liang, Jiaying Peng, Yang Liu, Jintang Li, Fenfang Xie, and Zibin Zheng. 2021. Phishing Scams Detection in Ethereum Transaction Network. *ACM Transactions on Internet Technology* 21: 1–16. [CrossRef]

Chen, Weili, Xiongfeng Guo, Zhiguang Chen, Zibin Zheng, and Yutong Lu. 2020. Phishing Scam Detection on Ethereum: Towards Financial Security for Blockchain Ecosystem. pp. 4506–12. Available online: https://www.ijcai.org/proceedings/2020/621 (accessed on 21 March 2022).

Chen, Weili, YueJin Xu, Zibin Zheng, Yuren Zhou, Jianxun Yang, and Jing Bian. 2019. Detecting "Pump & dump schemes" on cryptocurrency market using an improved apriori algorithm. Paper presented at the 13th IEEE International Conference on Service-Oriented System Engineering, SOSE 2019, San Francisco, CA, USA, April 4–9; pp. 293–98. [CrossRef]

Corbet, Shaen, Douglas Cumming, Brian Lucey, Maurice Peat, and Samuel A. Vigne. 2020. The Destabilising Effects of Cryptocurrency Cybercriminality. *Economics Letters* 191: 108741. [CrossRef]

Dika, Ardit, and Mariusz Nowostawski. 2018. Security Vulnerabilities in Ethereum Smart Contracts. Paper presented at the 2018 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, July 30–August 3; pp. 955–62. [CrossRef]

Fatima, Rubia, Affan Yasin Chouhan, Lin Liu, and Wang Jianmin. 2019. How persuasive is a phishing email? A phishing game for phishing awareness. *Journal of Computer Security* 27: 581–612. [CrossRef]

Froehlich, Michael, Philipp Hulm, and Florian Alt. 2021. Under Pressure. A User-Centered Threat Model for Cryptocurrency Owners. Paper presented at the 2021 4th International Conference on Blockchain Technology and Applications, Xi'an, China, December 17–19; pp. 39–50. [CrossRef]

Gottipati, Himani. 2020. A Proposed Cybersecurity Model for Cryptocurrency Exchanges. *Computer Science, Mathematics*. [CrossRef]

Holub, Artsiom, and Jeremiah O'Connor. 2018. COINHOARDER: Tracking a Ukrainian Bitcoin Phishing Ring DNS Style 2018. Paper presented at the 2018 APWG Symposium on Electronic Crime Research (eCrime), San Diego, CA, USA, May 15–17; pp. 1–5. [CrossRef]

Ivanov, Michael A., Bogdana V. Kliuchnikova, Ilya V. Chugunkov, and Anna M. Plaksina. 2021. Phishing Attacks and Protection against Them. Paper presented at the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2021, St. Petersburg, Moscow, Russia, January 26–29; pp. 425–28. [CrossRef]

Lal, Banwari, Rachit Agarwal, and Sandeep Shukla. 2021. Understanding Money Trails of Suspicious Activities in a cryptocurrency-based Blockchain. *arXiv* arXiv:2108.11818.

Lapuh Bele, Julija. 2021. Cryptocurrencies as facilitators of cybercrime. *SHS Web of Conferences* 111: 01005. [CrossRef]

Phillips, Ross, and Heidi Wilder. 2020. Tracing Cryptocurrency Scams: Clustering Replicated Advance-Fee and Phishing Websites. Paper presented at the IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, May 2–6; pp. 1–8. [CrossRef]

Poursafaei, Farimah, Ghaith Hamad, and Zeljko Zilic. 2020. Detecting Malicious Ethereum Entities via Application of Machine Learning Classification. Paper presented at the 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, September 28–30.

Reddy, Eveshnie. 2020. Analysing the investigation and prosecution of cryptocurrency crime as provided for by the South African cybercrimes bill. *Statute Law Review* 41: 226–39. [CrossRef]

Reddy, Eveshnie, and Anthony Minnaar. 2018. Cryptocurrency: A Tool and Target for Cybercrime. Available online: https://www.researchgate.net/publication/338572871 (accessed on 1 April 2022).

Sayeed, Sarwar, and Hector Marco-Gisbert. 2018. On the Effectiveness of Blockchain Against Cryptocurrency Attacks. Paper presented at the UBICOMM 2018: The Twelfth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, Athens, Greece, November 18–22; vol. 2018, pp. 9–14.

Șcheau, Mircea, and Ștefan Zaharie. 2018. The Way of Cryptocurrency. *Economy Informatics* 18: 32–44.

Shetewy, Nsreen, Jamal Aitlaadam, and Li Jun Jiang. 2019. Challenges of the Bitcoin in the Arabic Countries. *Journal of Economics and Sustainable Development* 10: 154–59. [CrossRef]

Trozze, Arianna, Josh Kamps, Eray ArdaAkartuna, Florian J. Hetzel, Bennett Kleinberg, Toby Davies, and Shane D Johnson. 2022. Cryptocurrencies and future financial crime. *Crime Science* 11: 1. [CrossRef] [PubMed]

Varlioglu, Said, Nelly Elsayed, Zag Elsayed, and Murat Ozer. 2022. The Dangerous Combo: Fileless Malware and Cryptojacking. Paper presented at the SoutheastCon 2022, Mobile, AL, USA, March 26–April 3; pp. 125–32.

Weber, Kristin, Andreas ESchütz, Tobias Fertig, and Nicholas H. Müller. 2020. Exploiting the human factor: Social engineering attacks on cryptocurrency users. In *Learning and Collaboration Technologies. Human and Technology Ecosystem*. Lecture Notes in Computer Science-Crime Science, 2022. Number 1. Cham: Springer, vol. 11, pp. 650–68. [CrossRef]

Wen, Haixian, Junyuan Fang, Jiajing Wu, and Zibin Zheng. 2021. Transaction-based hidden strategies against general phishing detection framework on ethereum. Paper presented at the IEEE International Symposium on Circuits and Systems, Daegu, Korea, May 22–28; pp. 1–5. [CrossRef]

Wu, Jiajing, Qi Yuan, Dan Lin, Wei You, Weili Chen, Chuan Chen, and Zibin Zheng. 2022. Who Are the Phishers? Phishing Scam Detection on Ethereum via Network Embedding. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 52: 1156–66. [CrossRef]

Xia, Pengcheng, Bingyu Zhang, Ru Ji, Bingyu Gao, Lei Wu, Xiapu Luo, Haoyu Wang, and Guoai Xu. 2020a. Characterizing Cryptocurrency Exchange Scams. *arXiv* arXiv:2003.07314. [CrossRef]

Xia, Pengcheng, Haoyu Wang, Xiapu Luo, Lei Wu, Yajin Zhou, Guangdong Bai, Guoai Xu, Gang Huang, and Xuanzhe Liu. 2020b. Don't Fish in Troubled Waters! Characterizing Coronavirus-themed Cryptocurrency Scams. *arXiv* arXiv:2007.13639.

Yuan, Qi, Baoying Huang, Jie Zhang, Jiajing Wu, and Haonan Zhang. 2020. Detecting Phishing Scams on Ethereum Based on Transaction Records. Paper presented at the 2020 IEEE International Symposium on Circuits and Systems (ISCAS), Seville, Spain, October 12–14; pp. 1–5. [CrossRef]